УДК 621.396:004.621.3

Капустян М.В., Хорошко В.А. (ГУИКТ)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОНТРОЛЯ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривается процесс контроля качества как последовательность отдельных операций. Рассмотрена задача оценки качества систем контроля в зависимости от качества контролируемых параметров методических и инструментальных ошибок средств контроля.

Ключевые слова: контроль качества, системы контроля, математическая модель, система защиты информации.

Введение. При проектировании средств и систем контроля безопасности, а также задачи предсказания ожидаемого успеха рациональной организации контроля с учетом влияния случайных факторов. Решение этих задач предполагает формализацию исследования процессов формирования решений при контроле, а для применения аналитических методов в этих исследованиях необходимо построение математической модели контроля, т.е. системы управления или операторов, описывающих зависимость выходных характеристик системы контроля (СК) от внешних и внутренних воздействий при функционировании их. С точки зрения предъявляемых требований к качеству контролируемых объектов (системы и подсистемы защиты информации, системы поддержки принятия решений, контроль качества функционирования противодействия несанкционированному получению информации), определение их качества, признак (физическая величина, совокупность физических величин, технические характеристики, обобщенный показатель и т.д.), θ может находится в одном из m возможных состояний.

При этом событие E_r, определение условия оптимального параметра (ОП) в r-м различимом состоянии запишется в виде

$$E_r : \{\theta \in (d_{r-1}; d_r)\}, \quad (1)$$

где d_{r-1}, d_r – соответственно нижняя и верхняя границы r-го состояния ОП.

С точки зрения исследования операций контроля, любое другое мероприятие (система действий), объединенное одним замыслом и направленное к достижению определенной цели, является операцией.

Операция контроля [1] определяется из элементарных операций (ЭО), выполняемых в определенной последовательности, и степень детализации определяется целью исследования и контроля. Процесс контроля (операция контроля) заключается в том, что ОП подвергается последовательному преобразованию. Заключение о принадлежности ОП к различному, с точки зрения контрольного эксперимента, состоянию проводится посредством разбраковки, т.е. сравнения результатов измерения преобразованного ОП с установленными границами различимых состояний.

Основная часть. При этом событие F_i, определяющее условие принятия решения с принадлежности ОП *i*-му состоянию, запишется в виде

$$F_i : \{Y \in (D_{i-1}; D_i)\}, \quad (2)$$

где Y – результат измерения преобразованного ОП; D_{i-1}, D_i - соответственно нижняя и верхняя границы *i*-го состояния преобразованного ОП.

Поскольку события E_r и F_i вследствие ошибок контроля могут не совпадать, то по результатам контроля ОП, находящегося в r-м состоянии, могут быть различимы m взаимно исключающих событий E_r F_i, $i = \overline{1,m}$.

Графически операция контроля r-го состояния ОП может быть представлена в виде стохастического графа (см. рис.1), в котором вероятности осуществления дуг соответствуют

условным вероятностям переходов, а вероятности реализации узлов – безусловным вероятностям событий.

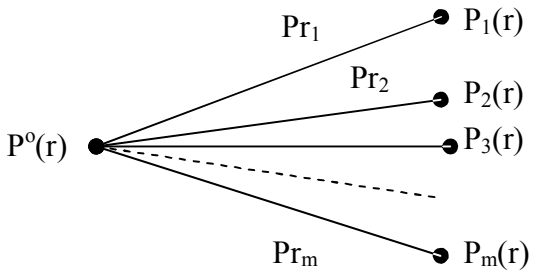

Рис.1. Стохастический граф

На основе рис.1 и логических рассуждений видно, что $p^{\circ}(\mathrm{r})=\mathrm{P}(\theta \in E_r)$ - вероятность нахождения ОП в состоянии r; $\mathrm{p_{ir}} = P(Y \in F_i / \theta \in E_r)$ - условная вероятность признается ОП по результатам контроля в i–м состоянии при условии, что он находится в r -м состоянии; $p_i(r) = P\begin{pmatrix} \theta \in E_r \\ Y \in F_i \end{pmatrix}$ - безусловная вероятность отнесения ОП, находящегося в r -м состоянии, к i-му.

На рисунке приняты следующие обозначения

$$P_i(r) = p^{\circ}(\mathrm{r})\mathrm{p_{ri}}\,. \tag{3}$$

Таким образом, качество контроля r -го состояния ОП полностью описывается вероятностью его нахождения в данном состоянии перед контролем и матрицей переходных вероятностей

$$\left\| p_{r1},...,p_{ri},...,p_{rm} \right\|. \tag{4}$$

Поскольку все сказанное относится к контролю любого из возможных состояний ОП, полученные результаты могут быть распространены на описание процесса контроля его остальных $m-1$ состояний. В связи с тем, что ОП, описанный по результатам контроля к i–му состоянию, перед контролем мог находиться в любом из m возможных состояний, то вероятность получить решение (ОП находится в i–м состоянии) вычисляется по формуле

$$P(F_i) = \sum_{r=1}^{m} p^{\circ}(\mathrm{r})\mathrm{p_{ri}}\,. \tag{5}$$

Таким образом, процесс контроля ОП может быть описан матрицей строкой вероятностей его различимых состояний перед началом контроля и матрицей переходных вероятностей

$$\begin{matrix} p_{11} & p_{12} & \cdots & p_{1j} & \cdots & p_{1m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{i1} & p_{i2} & \cdots & p_{ij} & \cdots & p_{im} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{m1} & p_{m2} & \cdots & p_{m2} & \cdots & p_{mm} \end{matrix}\,. \tag{6}$$

Показатели точности системы контроля. Одной из основных характеристик СК является точность. В дальнейшем под точностью СК будем понимать ее качество, отражающее близость к нулю ее ошибок, а под ошибками СК – отклонение результатов контроля от некоторых желаемых (идеальных). Понятие точности и ошибок СК, можно обобщить, включив в него любые отклонения от желаемого результата, в том числе и весьма существенные, связанные с частичным или полным ее отказом. Цель контроля ОП – определение состояния, в котором он находится. Ошибка СК в целом – это событие, заключающееся в отнесении, к некоторому i–му состоянию ОП, в действительности

находящегося в *j*-м состоянии. Очевидно, что матрица переходных вероятностей идеального (абсолютно точного) контроля должна быть единичной матрицей порядка m, т.е. $p_{rj}(r \neq j) = 0$, $p_{rj}(r = j) = 1$. Поскольку матрица переходных вероятностей содержит вероятности всех возможных при контроле ОП переходов как желаемых, так и нежелаемых, то она может служить показателем его точности, причем элементы матрицы $p_{r=j}$ характеризуют правильность (точность), а элементы $p_{r\neq j}$ - ошибки.

Математическая модель формирования решения при контроле качества. Для построения математической модели формирования решений при контроле качества, описывающей зависимости выходных характеристик СК от входных и внутренних воздействий, рассмотрим формирование решения при контроле как результат последовательного выполнения ряда ЭО, которые производят последовательное преобразование ОП, и в результате действия некоторой ЭО следующая операция воспринимает результат преобразования ОП всеми предшествующими ЭО [2].

Обозначим через θ^1, θ^2,…, θ^i, …, $\theta^N = N$ результаты преобразования ОП одной, двумя, …, *i*, …, *N* ЭО выполнения последовательно.

Рассмотрим преобразование ОП, находящегося в состоянии E_r, рядом последовательно выполняемых ЭО контроля. После выполнения $(k-1)$-й ЭО преобразований ОП θ^{k-1} может находиться в любом из *m* возможных состояний. Обозначим безусловную вероятность нахождения преобразованного ОП в *i*-м состоянии после завершения $(k-1)$-й ЭО через $P_i^{(k-1)}(r)$, при этом:

$$P_i^{(k-1)}(r) = p\begin{pmatrix} \theta^{k-1} \in E_i^{k-1} \\ \theta \in E_r \end{pmatrix}, \tag{7}$$

где E_i^{k-1} - *i*-е из *m* возможных состояний преобразованного ОП после завершения $(k-1)$-й ЭО.

Аналогично для *k*-й ЭО:

$$P_j^k(r) = p\begin{pmatrix} \theta^k \in E_j^k \\ \theta \in E_r \end{pmatrix}. \tag{8}$$

Преобразованный ОП, находящийся после выполнения *k*-й ЭО в состоянии E_j^k, в начале ее, т.е. после завершения $(k-1)$-й ЭО, мог находиться в любом из возможных состояний. Тогда:

$$P_j^k(r) = \sum_{i=1}^{m} p_i^{k-1}(\mathrm{r}) p_{ij}^{k}(r), \tag{9}$$

где $p_{ij}^k(r)$ - условная вероятность перехода преобразованного ОП из состояния E_i^{k-1} в состояние E_j^k при выполнении *k*-й ЭО, т.е.:

$$P_{ij}^k(r) = p\begin{pmatrix} \theta^k \in E_j^k / \theta^{k-1} \in E_i^{k-1} \\ \theta \in E_r \end{pmatrix}, \tag{10}$$

k-я ЭО при контроле *r*-го состояния ОП может быть описана матрицей строкой безусловных вероятностей состояний перед началом ее действия и матрицей переходных вероятностей:

$$\left\| \begin{matrix} p_{11}^k(r) & \dots & p_{1j}^k(r) & \dots & p_{1m}^k(r) \\ \dots & \dots & \dots & \dots & \dots \\ p_{i1}^k(r) & \dots & p_{ij}^k(r) & \dots & p_{im}^k(r) \\ \dots & \dots & \dots & \dots & \dots \\ p_{m1}^k(r) & \dots & p_{mj}^k(r) & \dots & p_{mm}^k(r) \end{matrix} \right\|. \qquad (11)$$

Матрица переходных вероятностей (11) – квадратная матрица порядка m с неотрицательными элементами, сумма элементов каждой строки равна единице, т.е.

$$\sum_{i=1}^{m} p_{ij}^k(r) = 1. \qquad (12)$$

Как следует из выражения (9), матрица-строка безусловных вероятностей на выходе k-й ЭО – произведение матрицы-строки безусловных вероятностей на ее входе на квадратную матрицу переходных вероятностей.

Первая ЭО при контроле r-го состояния ОП полностью описывается безусловной вероятностью r-го состояния ОП $p^{\circ}(\mathrm{r})$ и матрицей-строкой переходных вероятностей:

$$\left\| p_{r1}^1(r) \dots p_{rj}^1(r) \dots p_{rm}^1(r) \right\|. \qquad (13)$$

Безусловные вероятности состояний на выходе первой ЭО определяется выражением:

$$p_j^1(r) = p^{\circ}(\mathrm{r})\, p_{rj}^1(r), \; j = \overline{1,m}. \qquad (14)$$

Последовательно выполняемые n ЭО можно заменить одной эквивалентной операцией, для которой матрица переходных вероятностей – есть произведение матриц переходных вероятностей всех ЭО, т.е.:

$$P_{ij}^{(k,k+n)}(r) = \sum_{\nu_1=1}^{m} \sum_{\nu_2=1}^{m} \dots \sum_{\nu_n=1}^{m} p_{1\nu}^k(r)\, p_{\nu_1\nu_2}^{k+1} \dots p_{\nu_{n-1}}^{k+n}. \qquad (15)$$

Таким образом, если известна матрица-строка безусловных вероятностей в начале некоторой ЭО и матрицы переходных вероятностей последующих операций, безусловные вероятности состояний ОП на выходе последней ЭО определяется по формуле, аналогичной (8), т.е.:

$$P_j^{(k,k+n)}(r) = \sum_{i=1}^{m} p_i^k(r)\, p_{1j}^{(k,k+n)}(r), \qquad (16)$$

причем переходные вероятности $P_{ij}^{(k,k+n)}$ определяются по формуле (15).

Безусловные вероятности состояний на выходе операции контроля определяются из выражения:

$$P_j(r) = P_j^n(r) = P^{\circ}(\mathrm{r}) \mathrm{P}_{\mathrm{rj}}^{(1,\mathrm{n})}(r), \qquad (17)$$

$$\mathrm{P}_{\mathrm{rj}}^{(1,\mathrm{n})}(r) = \sum_{i=1}^{m} p_{ri}^1(r)\, p_{ij}^{(2,n)}(r), \qquad (18)$$

$p_{ri}^1(r)$ - переходные вероятности первой ЭО;

$p_{ij}^{(2,n)}(r)$ - эквивалентные переходные вероятности последующих ЭО, определяемые по выражению (15).

Поскольку все сказанное относится к контролю любого r-го состояния ОП, полученные результаты распространяются на контроль остальных (n-1) состояний ОП.

Таким образом, для определения операции контроля, т.е. определения вероятности состояний преобразованного ОП на ее выходе, необходимо знать вероятности состояний ОП на ее входе и переходные вероятности каждой из ЭО составляющих операцию контроля, для вычисления которых необходимо знать характеристики погрешностей выполнения этих операций.

Для определения переходных вероятностей ЭО рассмотрим некоторую (пусть *k*-ю) ЭО при контроле *r*-го состояния ОП. Данная операция осуществляет некоторое преобразование информации, полученной после преобразования ее предшествующими ЭО, причем действительное преобразование не соответствует требуемому преобразованию из-за несовершенства выбранных методов и средств контроля, реализующих ее, что приводит к возникновению ошибок преобразования. Если бы ошибки преобразования отсутствовали, данная ЭО переводила бы преобразованный ОП в то состояние, в котором она его воспринимала, и тогда матрица переходных вероятностей представляла бы собой единичную матрицу, где $P_{ij}^{k}=1$ при $i=j$ и $P_{ij}^{k}=0$ при $i\neq j$.

Для реальной ЭО матрица переходных вероятностей отличается тем больше от единичной, чем больше ошибки преобразования, т.е. она характеризует точность ЭО. При исследовании погрешности ЭО, следует иметь в виду две стороны этого вопроса [3], во-первых, способность ЭО выполнять необходимое преобразование ОП при ее идеальной реализации средствами контроля; во-вторых, потерю (искажение) информации, связанную с погрешностью средств, реализующих ЭО. Первой соответствует методическая ошибка, вторая сторона характеризует инструментальную ошибку ЭО.

Для определения влияния методической и инструментальной составляющих ошибок преобразования ЭО на ее переходные вероятности рассмотрим некоторую (пусть *k*-ю) ЭО при контроле *r*-го состояния ОП. В соответствии с выражением (8) имеем

$$P_{ij12}^{(k,k+1)}(r)=\sum_{\nu=1}^{m}p_{i\nu 1}^{k}(r)\,p_{j\nu 2}^{k+1}(r), \qquad (19)$$

где $P_{ij12}^{(k,k+1)}(r)$ - условная вероятность перехода преобразования ОП из *i*-го состояния в j-е при последовательном действии двух ошибок преобразования; $p_{i\nu 1}^{k}(r)$ и $p_{j\nu 2}^{k+1}(r)$ - условная вероятность перехода преобразованного ОП из *i*-го состояния в j-е при действии первой (второй) в данной последовательности действия из двух ошибок преобразования. При подставлении в формулу (19) вместо индексов 1 и 2 соответственно индексы *M* (методическая составляющая погрешности преобразования) в завсимости от последовательности их действия определяются условные вероятности перехода преобразованного ОП из *i*-го состояния в j-е при совместном действии методических и инструментальных составляющих погрешностей преобразования ЭО. Поскольку все сказанное относится к контролю *r*-го состояния ОП, полученные результаты распространяются на контроль остальных *m-1* состояний ОП.

Выводы. Рассмотренная математическая модель формирования решения при контроле позволяет при известных характеристиках ОП системы, реализующих ЭО контроля, определить вероятности состояний преобразованного ОП на выходе последней ЭО при контроле любого из возможных состояний контролируемой системы и тем самым оценить степень приспособленности операции контроля к выполнению стоящей перед нею задачи или ее эффективность. Модель позволяет оценить влияние любой отдельно взятой ЭО на результаты контроля и рациональным образом выбрать ее характеристики.

Литература

1. Пархуць Л.Т. – Нестационарные модели систем информационного обеспечения процессов защиты объектов / Пархуць Л.Т., Хорошко В.А. // Сб.науч.трудов НАУ «Защита информации», спецвыпуск, 2008. – С.204-228.

2. Браиловский Н.Н. – Система автоматизации программирования процессов оценки технического состояния систем защиты / Браиловский Н.Н., Орленко, В.С., Хорошко В.А. // Управління розвитком, №15, 2008. –С.38-40.

3. Андреев В.И. – Количественная оценка защищенности технических объектов с учетом их функционирования / Андреев В.И., Козлов В.С., Хорошко В.А. // Захист інформації, №2, 2004. С.47-51.

Надійшла: 18.06.2011 р.

Рецензент: д.т.н., проф. Куц Ю.В.